UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/626,420	07/24/2003	Sheueling Chang Shantz	6000-32301	9856

58467 7590 12/18/2007

MHKKG/SUN
P.O. BOX 398
AUSTIN, TX 78767

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	**PAPER NUMBER**
2136	
MAIL DATE	**DELIVERY MODE**
12/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/626,420	**Applicant(s)** SHANTZ ET AL.	
	Examiner Carlton V. Johnson	**Art Unit** 2136	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 20 November 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: 1-65.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

Continuation of 11. does NOT place the application in condition for allowance because: Response to Arguments

Applicant's claim limitations disclose the completion of arithmetic operations (addition, subtraction, multiplication) with regular and extended registers. Each type of arithmetic operation disclosed by applicants claim invention is disclosed by the Gressel and Stribaek prior art references.

The operations of addition, subtraction, and multiplication, XOR operations are arithmetic operations well known in the art. The performance of these arithmetic operations is the basis of the functions performed by computer systems and Information Technology systems. There is nothing novel or unique about the completion of these operations. In the processing of arithmetic operations, the reuse of the results (full word, partial word) of a first arithmetic operation as input to a second arithmetic operation is well known in the art. There is nothing novel or unique about the reuse of a result (full word, partial word) from one operation as input to a second operation. The operation of multiple instructions within a single combined instruction is well known in the art. There is nothing novel or unique about this particular structure for an arithmetic instruction. The arithmetic operation, XOR, is a standard operation performed by a computer system. There is nothing novel or unique about this particular arithmetic operation.
All of the arithmetic operations disclosed by applicant's invention are well known in the art. There is nothing novel or unique

Applicants claimed invention is 65 claims which are merely a series of arithmetic operations. Nowhere does applicant designate what tangible result is created from the completion of these arithmetic operations. Claims 1, 18, 57, 61, 64, and 65 were amended to indicate the mention of a cryptographic application which can result in anything from key generation, key revocation, digital signature generation, hash generation, digital certificate generation, message digest generation, and etc. The specification mentions the acceleration of the generation of a cryptographic key. The cryptographic application can be any of a large number of cryptographic processing applications. But, the claimed invention does not mention the word key anywhere. Therefore, the arithmetic operations in the claimed invention must not be used to accelerate the generation of a cryptographic key. In any event, the Gressel prior art discloses the acceleration of arithmetic operations by the prior art invention. (see Gressel col. 1, lines 39-45; col. 5, lines 23-25: arithmetic operation acceleration) In addition, the Gressel prior art discloses that the arithmetic operations can be utilized for the generation of cryptographic keys as per the specification and the processing of a cryptographic application as per claim limitations. (see Gressel col. 3, lines 24-35: cryptographic application (cryptographic key generation, accelerated))

The Gressel prior art discloses arithmetic operations such as multiplication and addition utilizing the partial results of the first operation. (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 2, lines 31-37: multiplication two values, summing two values utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication)

In very long instruction word (VLIW) architectures, which include many microcode architectures, multiple simultaneous operations and operands are specified in a single instruction. (http://www.answers.com/topic/instruction-computer-science) This standard computer architecture feature discloses a single arithmetic instruction to perform multiple operations.

An instruction also designates the destination address (memory locations, registers) for the results of the completion of an instruction. ("On traditional architectures, an instruction includes an opcode specifying the operation to be performed, such as "add contents of memory to register", and zero or more operand specifiers, which may specify registers, memory locations, or literal data ": http://www.answers.com/topic/instruction-computer-science)

The Gressel prior art discloses partial results from an arithmetic operation. The partial results could be the high order bits. (see Gressel col. 2, lines 31-37: arithmetic operations utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication) A partial result is the high or low order bits from a word.

The Gressel prior art discloses storing and utilizing the results of an operation in subsequent arithmetic operations. (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into a next (subsequent) operation)

The examiner has considered the applicant's remarks concerning a cryptographic application executing arithmetic instructions; a first number is multiplied by a second number, and a partial result from a previously executed arithmetic instruction is added to generate a result that represents the first number multiplied by the second number summed with the partial result from a previously executed single arithmetic instruction; the high order portion of the generated result is saved in an extended carry register as a next partial result for use with execution of a subsequent single arithmetic instruction. Applicant's arguments have thus been fully analyzed and considered but they are not persuasive.

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of Gressel (6,748,410) and Stribaek (7,181,484) discloses the applicant's invention. .

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12/17/07